AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Chad Albin, Detective with the Lee's Summit Missouri Police Department ("LSPD"), Lee's Summit, Missouri, being duly sworn, depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of property, to wit: a black Apple iPhone in a black/clear case, ("TARGET DEVICE 1") (further described in Attachment A-1), an Apple iPad in a black case ("TARGET DEVICE 2") (further described in Attachment A-2), a silver Microsoft laptop with serial number 064606602154 ("TARGET DEVICE 3") (further described in Attachment A-3), an external hard drive, storage size 1TB ("TARGET DEVICE 4") (further described in Attachment A-4), and an external hard drive, storage size 2 TB ("TARGET DEVICE 5") (further described in Attachment A-5), collectively referred to as the "TARGET DEVICES," and to search for and seize therefrom the information further described in Attachment B. The TARGET DEVICES were lawfully seized pursuant to an investigation by investigators with LSPD, on December 19 and 20, 2024, as further described below. The TARGET DEVICES are currently securely located at LSPD Headquarters, 10 NE Tudor Road, Lee's Summit, Missouri 64086.

2. I have been employed as a Detective for LSPD since November 2007. As part of my duties as a Detective, I am assigned to investigate violations of municipal, state, and federal law, specifically regarding the online exploitation of children. This includes violations pertaining to illegal possession, receipt, transmission, and production of material depicting the sexual exploitation of minors. I have had numerous hours of professional law enforcement training in the

detection and investigation of criminal offenses. I have written, executed, and/or participated in the execution of numerous search warrants. Specifically pertaining to the area of child pornography and child exploitation investigations, I have gained expertise in these investigations through training, discussions with other law enforcement officers, and everyday work related to conducting these types of investigations. I have also served as a federally deputized Task Force Officer with the United States Secret Service since 2010. The sponsoring and host agency for the task force is the U.S. Secret Service Field Office in Kansas City, Missouri. The Cyber Crime Task Force focuses on financial crimes and computer-related offenses, including Internet Crimes Against Children ("ICAC") cases involving Child Sexual Abuse Material ("CSAM").

3. This affidavit is based upon information I have gained from my investigation as well as my training and experience. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe evidence, fruits, and instrumentalities of the violation of Title 18 U.S.C. § 2252 (Distribution, Receipt, and Possession of Child Pornography), are presently located on the TARGET DEVICES.

4. At all times throughout this affidavit, I use the term "child pornography" and "Child Sexual Abuse Material" interchangeably merely as shorthand to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms "visual depiction," "minor," and "sexually explicit conduct" as those terms are defined in 18 U.S.C. § 2256 (See Definition Section below).

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18 U.S.C. § 2252.

a. 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving or distributing any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, if the producing of such a visual depiction involves the use of a minor engaging in sexually explicit conduct, and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252(a)(4)(B) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, material which contains any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct, and such visual depiction is of such conduct.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. On September 8, 2024, Media Lab/Kik generated an online Cyber Tip that was submitted to the National Center for Missing and Exploited Children ("NCMEC"). The Cyber Tip noted that the suspect identified by their Kik screen/username as "**kingbonbon00"** uploaded multiple images of child pornography via Kik Messenger. The display name on Kik Messenger was King Bonbon. The profile for "**kingbonbon00**" was associated to a home email address of sbrummond@gmail.com. The suspect uploaded twelve (12) videos of apparent child pornography

to a messaging group in Kik Messenger from the IP address 104.51.118.213 on September 8, 2024. The Cyber Tip report indicated that the Electronic Service Provider ("ESP"), Media Lab/Kik, had viewed the uploaded videos prior to submitting the report to NCMEC.

7. LSPD Investigators reviewed the videos that were the subject of the Cyber Tip report and determined that they contained content depicting child pornography. A sampling of the videos includes the following:

a. File 0f1a8 depicted two apparent prepubescent females completely nude engaging in sexually explicit conduct;

b. File 806f68 depicted a prepubescent female performing oral sex on an adult male penis; and

c. File 96f44b depicted two nude prepubescent females. One of females is performing oral sex on an adult male penis.

8. LSPD investigation developed **Seth BRUMMOND** ("**BRUMMOND**") as the subscriber of IP address 104.51.118.213 and eventually as the suspect in the Cyber Tip Report. **BRUMMOND** is a teacher at Lee's Summit West High School and resides at 1309 Rolling Drive, Greenwood, Missouri 64034, both locations being within the Western District of Missouri.

9. On December 18, 2024, federal search warrants were issued authorizing a search of the residence at 1309 Rolling Drive, Greenwood, Missouri 64034 (Case No. 24-SW-00694-WBG) and for **BRUMMOND'S** person (Case No. 24-SW-00695-WBG). On the morning of December 19, 2024, LSPD officers executed both aforementioned federal search warrants. At approximately 0555 hours, on December 19, 2024, LSPD Detectives conducted surveillance on **BRUMMOND** prior to serving the search warrants. **BRUMMOND** was observed leaving his

residence and LSPD officers followed **BRUMMOND** from his residence into Lee's Summit. After 0600 hours, an investigative stop was conducted and **BRUMMOND** was placed in custody. During the encounter with **BRUMMOND,** an iPhone was located in the vehicle that he had been driving. A federal search warrant (Case No. 24-SW- 00698-WBG) was issued authorizing a search of that iPhone that had been recovered from his vehicle.

10. During a *Mirandized* recorded interview of **BRUMMOND**, he admitted that he had used Kik Messenger to share child pornography during the time alleged in the Cyber Tip and that investigators would find "a lot" of child pornographic material in the iPhone that was seized from his vehicle. (Note: A preliminary review of the iPhone found in **BRUMMOND's** vehicle, pursuant to the search warrant, located a collection of at least approximately 200 photographs and videos depicting child pornography on the device.) Additionally, during the defendant's interview, he also stated that he had a laptop computer **(TARGET DEVICE 3)** in his office at his place of employment (Lee's Summit West High School).

11. School administrators at Lee's Summit West High School, after learning of **BRUMMOND'S** arrest, recovered **TARGET DEVICES 1, 2 and 3** from **BRUMMOND'S** office at the school. School administrators turned **TARGET DEVICES 1, 2, and 3** over to LSPD Detectives. **BRUMMOND** was subsequently questioned again, after being reminded of his rights, and acknowledged that the iPhone **(TARGET DEVICE 1)** and iPad **(TARGET DEVICE 2)** that were recovered from his office with the laptop **(TARGET DEVICE 3)** were all his, but that he had forgotten about **TARGET DEVICE 1 and 2**. LSPD Detectives later learned that there were also two external hard drives (**TARGET DEVICES 4 and 5**) in **BRUMMOND'S** personal

bag in his work office. Those devices were also provided to LSPD investigators by the school administrators in anticipation of the issuance of a search warrant. The **TARGET DEVICES** have been secured into evidence storage at LSPD Headquarters, 10 NE Tudor Rd, Lee's Summit, Missouri 64086.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

12. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

13. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

14. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer

to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

15. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers, to include external hard drives and thumb drives, has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

16. A smartphone, or smart phone, is a mobile phone with more advanced computing capability and connectivity than basic feature phones. Early smartphones typically combined the features of a mobile phone with those of another popular consumer device, such as a personal digital assistant (PDA), a media player, a digital camera, or a GPS navigation unit. Modern smartphones include all of those features plus the features of a touchscreen computer, including web browsing, Wi-Fi capability, and apps. Frequently, smartphones also include removable storage devices, or SD cards, where users can store data, including picture and video files.

17. Smart phone technology has expanded computer capability in recent years by allowing users to access the Internet via their phone. The smart phone user can search the Internet for specific files, check personal email accounts, log on to social networking sites, communicate with other computer users, compose and edit documents, and store and view movie and picture files. Affiant is aware of numerous Cloud based applications widely available online. These applications allow a user to sign up for an account which can be accessed by numerous devices including smart phones, tablets, and computers. These devices are capable of sharing data

contained within the Cloud including but not limited to images, videos, documents and programs via Wi-Fi or a cellular network. Affiant knows that forensic exams on electronic devices such as smart phones, tablets, and computers are capable of demonstrating connections to Cloud based applications and such devices frequently contain shared media. It is not uncommon to find the same images on multiple devices and on the Cloud. Images can also be transferred from a mobile device to a computer through a wired connection.

18. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

19. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

20. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained

unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

DEFINITIONS

21. The following definitions apply to this Affidavit and **Attachment B**:

a. "Child Erotica," as used herein, means materials that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

d. The "Internet" is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail").

e. "Internet Protocol address" or "IP address", as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the Internet service provider assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static if an Internet service provider assigns a user's computer a particular IP address each time the computer accesses the Internet.

f. "Logs" or "log files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, log on/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

g. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

h. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

i. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals or pubic areas of any person.

j. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

k. "Wireless telephone, cellphone, smartphone, or mobile phone" is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. A smartphone user may perform these various functions through software applications ("apps") which may store evidence of such use on the device.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

22. Based upon your Affiant's knowledge, training and experience, and the experience of other law enforcement personnel, I know that electronic devices, including **TARGET**

DEVICES, can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. As further described in **Attachment B**, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **TARGET DEVICES** were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **TARGET DEVICES** because:

a. Computers, cellphones, external hard drives, and thumb drives can serve as storage mediums and can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he or she might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

c. Forensic evidence on a device can also indicate who has used or controlled the **TARGET DEVICES** . This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

d. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how **TARGET DEVICES** were used, the purpose of its use, who used it, and when.

e. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or cell phone is evidence may depend on other information stored on the computer or cell phone and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

g. I know that when an individual uses a computer or cellphone to possess, or traffic over the Internet child pornography images, the computer or cellphone will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a device used to commit a crime of this type may contain:

data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

24. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **TARGET DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant. Additionally, if necessary, the warrant permits any electronic devices to be moved across state lines if necessary to conduct a forensic download the devices.

25. *Manner of Execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

26. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

a. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text

that do not rise to the level of child pornography, but which nonetheless fuel their deviant sexual fantasies involving children.

b. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

c. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

d. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

e. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes or other secure location.

CONCLUSION

27. Based on the foregoing, your Affiant respectfully submits that there is probable

cause to believe that evidence of violations of 18 U.S.C. § 2252, that is distribution, receipt, and possession of child pornography, will be found on the **TARGET DEVICES**. Your Affiant therefore respectfully requests that a search warrant be issued authorizing LSPD, with the appropriate assistance from other law enforcement officers, to search the **TARGET DEVICES**, more fully described in **Attachments A-1 through A-5**, and to search for and to seize therefrom, the items listed in **Attachment B**, which is property that constitutes evidence, fruits, and instrumentalities of the distribution, receipt and possession of child pornography.

Detective C. Albin, Badge #9919

Chad Albin
Task Force Officer
United States Secret Service

Subscribed and sworn to me via telephone this 13th day of January, 2025.

Via telephone at 5:48 pm

HONORABLE W. Brian Gaddy
United States Magistrate Judge
Western District of Missouri